

REMARKS/ARGUMENTS

1. The Applicant has carefully considered the official communication dated January 22, 2008. Applicant respectfully submits that the amendment and the following remarks are fully responsive to the official communication.
2. The claims have been amended in a minor fashion as indicated, with a view of improving the reader's understanding of the claimed invention. It is submitted that no new matter has been added as a result of the amendment.
3. With regard to paragraph 1 of the Detailed Action, we enclose an oath in which Applicant claims priority to US 6,442,525, as US 6,745,331 is a continuation of US 6,442,525.
4. In paragraph 4 of the Detailed Action, the Examiner alleges that the specification fails to comply with the enabling requirement. In particular, the Examiner alleges that "the detailed description does not disclose how exactly the authentication works".
5. We direct the Examiner to paragraphs 424 to 431 of US 20040172532 (i.e. the published version of the present application) which clearly outlines the seven step authentication process with reference to Figure 6. The process culminates at step 7 where "if the response 65 is 1, then Chip A 20 is considered authentic. If 0, Chip A 20 is considered invalid." Applicant submits that this is how the authentication process works and that there is ample information for the skilled person to implement this clearly laid out process.
6. In paragraph 4 of the Detailed Action, the Examiner alleges that "the limitation that the encrypted data is defined by two keys shared by the apparatus for decryption of the data, is new matter". Applicant respectfully disagrees as this feature was originally disclosed in the specification as explained below.
7. With regard to claim 1, it is clear from the wording "another integrated circuit of the apparatus" that the claimed "apparatus" includes the other integrated circuit. Referring to Figure 6 of US 20040172532, the claimed apparatus includes both System 21 and the other integrated circuit Chip T 23. As explained in paragraph 412 of US 20040172532, "integration of Chip T into System may be desirable". Returning to Figure 6, it is clear that secret keys K_T and K_A are shared by both System 21 and the other integrated circuit Chip T 23 that together form the apparatus. In particular, the external functions $E_{K_T}[R]$ in signal 61 and $E_{K_A}[R|M]$ in signal 64 are generated using secret keys K_T and K_A respectively, and these secret keys are clearly shared by the apparatus. These features were originally disclosed and do not constitute new matter.
8. In paragraph 7 of the Detailed Action, the Examiner alleges that claims 1 and 7 fail to particularly point out and distinctly claim subject matter which the applicant regards as the invention. As explained in the previous paragraph, the claimed "apparatus" includes both System 21 and the other integrated circuit Chip T 23. Referring to US 20040172532, the key K_T is a public key (see paragraph 423) used

to decrypt (see paragraph 430 where decryption function $D_{KT}[E_{KA}[R|M]]$ is evoked) an encrypted random number R (i.e. $E_{KA}[R|M]$) generated by another integrated circuit (i.e. Chip T 23, see paragraph 425). We submit that it is clear how the public key K_T is used.

9. In paragraph 10 of the Detailed Action, the Examiner alleges that “the disclosed invention is inoperable and therefore lacks utility” and that “no authentication actually takes place”. Once again, we direct the Examiner to paragraphs 424 to 431 of US 20040172532 which clearly outlines the seven step authentication process with reference to Figure 6. The process culminates at step 7 where “if the response 65 is 1, then Chip A 20 is considered authentic. If 0, Chip A 20 is considered invalid.” Applicant submits that the present invention clearly has utility.
10. Furthermore, Applicant submits that the claims adequately define the invention for which protection is being sought. Contrary to the Examiner’s assertion, the claims do not “merely disclose a memory with data on it”. Instead, the claims define that the encrypted data on the memory space is defined by a MAC which is formed in accordance with the novel and inventive procedure defined by the claims (i.e. using the two secret keys).
11. We respectfully disagree with the Examiner’s reasoning in paragraph 11 of the Official Action that the Official Action dated January 22, 2008 be made FINAL. MPEP 706.07(a) states that “*Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant’s amendment of the claims nor based on information submitted in an information disclosure statement filed during the period set forth in 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p)*”.
12. The Examiner has introduced a new ground of rejection in the form of 35§101 that is neither necessitated by applicant’s amendment of the claims nor based on information submitted in an information disclosure statement. Accordingly, the foregoing exception of MPEP 706.07(a) applies and the Official Action dated January 22, 2008 should clearly not be made FINAL.

It is respectfully submitted that all of the Examiner's objections have been successfully traversed. Accordingly, it is submitted that the application is now in condition for allowance. Reconsideration and allowance of the application are courteously solicited.

Very respectfully,

Applicant/s:



Kia Silverbrook

C/o:

Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email:

kia.silverbrook@silverbrookresearch.com

Telephone:

+612 9818 6633

Facsimile:

+61 2 9555 7762